www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, version 4 October 2016 T-CY(2016)11

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #11 (DRAFT)
Aspects of Terrorism
covered by the Budapest Convention

Proposal prepared by the T-CY Bureau
for consideration by the 16th Plenary of the T-CY (14-15 November 2016)

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses how different Articles of the Convention could apply to terrorism.

Many countries are Parties to numerous treaties, and subject to UN Security Council Resolutions, that require criminalization of different forms of terrorism, facilitation of terrorism, support for terrorism, and preparatory acts. In terrorism cases, countries often rely on offenses that derive from those topic-specific treaties, as well as additional offenses in national legislation.

The Budapest Convention is not a treaty that is focused specifically on terrorism. However, the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

The scope and limits are defined by Articles 14.2 and 25.1 Budapest Convention:

> Article 14.2
> 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
> a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
> b other criminal offences committed by means of a computer system; and
> c the collection of evidence in electronic form of a criminal offence.
>
> Article 25.1
> "The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

See also Articles 23 and 27.1 Budapest Convention as well as other Guidance Notes, such as the Guidance Notes on critical infrastructure attacks or distributed denial of service attacks.

2 Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

2.1 Procedural provisions

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of case, as Article 14 provides.

[1] See the mandate of the T-CY (Article 46 Budapest Convention).

In fact, the specific procedural measures can be very useful, for example in terrorism cases, if a computer system was used to commit or facilitate the offence or if the evidence of that offence is stored in electronic form or if a suspect can be identified through subscriber information, including an Internet Protocol address. Thus, in terrorism cases, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

2.2 International mutual legal assistance provisions

The Convention's international cooperation powers (Articles 23-35) are of similar breadth.

Thus, Parties must make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools, as well as other international cooperation provisions, in order to cooperate with other Parties in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

2.3 Substantive criminal law provisions

Finally, as noted above, terrorists and terrorist groups may carry out acts criminalized by the Convention as part of achieving their goals.

Relevant Articles	Examples
Article 2 – Illegal access	A computer system may be illegally accessed to obtain personally identifiable information (e.g. information about government employees to target them for attack).
Article 3 – Illegal interception	Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain information about a person's location (e.g. to target that person).
Article 4 – Data interference	Computer data may be damaged, deleted, deteriorated, altered, or suppressed (e.g. a hospital's medical records can be altered to be dangerously incorrect, or interference with an air traffic control system can affect flight safety).
Article 5 – System interference	The functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).
Article 6, Misuse of devices	The sale, procurement for use, import, distribution or other acts making available of computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate a terrorist attack (e.g. it can lead to damage to a country's electrical power grid).
Article 7, Computer-related forgery	Computer data (for example the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8, Computer-related fraud	Computer data may be input, altered, deleted, or suppressed, and/or the function of a computer system may be interfered with, causing other persons to lose property (for example, an attack on a country's banking system can cause loss of property to a number of victims).
Article 11 – Attempt, aiding and abetting	Crimes specified in the treaty may be attempted, aided or abetted in furtherance of terrorism.
Article 12 – Corporate liability	Crimes covered by Articles 2-11 of the Convention in furtherance of terrorism may be carried out by legal persons who would be liable under Article 12.

Article 13 – Sanctions	Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against systems that are crucial to daily life, for example public transport, banking systems or hospital infrastructure. The effects may differ in different countries, depending also on their degree of interconnectedness and their dependence on such systems. A Party may provide in its domestic law a sanction that is unsuitably lenient for terrorism-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". Parties may also consider aggravating circumstances, for example if such acts affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

Other crimes covered by the Convention but not mentioned specifically above, including the production of child exploitation materials or trafficking in stolen intellectual property, may also be carried out in connection with terrorism.

For Parties to the Budapest Convention which are also Parties to the Additional Protocol on Xenophobia and Racism Committed Through Computer Systems (ETS 189)[2], two articles of the Protocol are relevant as these may relate to radicalisation and violent extremism which may lead to terrorism. These are Article 4 of the Protocol covering racist and xenophobic motivated threat and Article 6 covering denial, gross minimisation, approval or justification of genocide or crimes against humanity.

3 T-CY statement

The T-CY agrees that the substantive crimes in the Convention may also be acts of terrorism as defined in applicable law.

The substantive crimes in the Convention may be carried out to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

The procedural and mutual legal assistance tools in the Convention may be used to investigate terrorism, its facilitation, support for it, or preparatory acts.

[2] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189